fasthosts ProActive

Shadow IT

What is it and how can it affect you?

Shadow IT refers to the use of IT systems, software, applications, or services in an organisation without the approval or knowledge of the IT department. These unofficial IT practices are usually used by employees or departments looking for solutions that meet their specific needs quickly or get around perceived internal red tape. Common examples of shadow IT include using unauthorised cloud storage services and unsanctioned software applications.

How can shadow IT affect your TCO?

The term "shadow" is a pretty accurate description. It implies that these IT activities are sneaky, operating outside of the direct view and control of the IT department, which is exactly what they are. This makes them difficult to monitor and manage effectively.

While the intentions behind shadow IT might be to improve productivity and innovation, it can have various negative impacts on an organisation, particularly in terms of the Total Cost of Ownership (TCO). For example:

- **Duplicate investments**: Shadow IT often leads to duplication of resources and services. Different departments or teams might unknowingly invest in similar or overlapping IT solutions, meaning wasted spending on licences, hardware, or subscriptions.
- **Integration challenges:** Shadow IT systems aren't designed to be part of the organisation's overall IT infrastructure. Because of this, they might lack proper integration with existing systems, leading to data silos, compatibility issues, and additional expenses to connect different applications.
- **Security and compliance risks:** Unsanctioned IT solutions might not follow the organisation's security standards or compliance requirements. This can expose the company to potential data breaches, legal liabilities, and financial losses related to cyber incidents.
- **Support and maintenance costs:** The IT department is responsible for providing support and maintenance to officially approved systems. When shadow IT applications are used, IT staff may need to spend extra time and effort troubleshooting issues they aren't familiar with, increasing operational costs.
- **Lack of scalability:** Shadow IT solutions may not be scalable to meet the entire organisation's needs. As the company grows, these ad-hoc systems might struggle to keep up, leading to inefficiencies and the need for expensive upgrades or replacements.

- **Vendor management challenges:** Managing relationships with multiple IT vendors starts to get tricky when different departments independently talk to their preferred providers. This can lead to inadequate contracts, pricing, and reduced negotiation leverage.
- **Loss of control:** Shadow IT can lead to a loss of control over the organisation's overall IT environment. This lack of visibility can hinder strategic decision-making and governance, making it difficult to optimise IT resources effectively.

How can we help prevent shadow IT and the growing bill that comes with it?

To address shadow IT's negative impacts on TCO, organisations should focus on having open conversations with employees. Communication is key. Encouraging employees to share their technology needs and concerns with the IT department leads to a better understanding and more effective solutions that fit with the organisation's overall goals and reduce TCO.

Can a fully-managed MSP reduce the risk from shadow IT?

Yes! Using a fully-managed Managed Service Provider (MSP) can significantly reduce the risk from shadow IT by providing infrastructure management, support, and security solutions. Here are some more examples of how a fully-managed MSP can help with Shadow IT:

- **Control and visibility:** A reputable MSP will have the tools and expertise to monitor and manage your infrastructure. This control lets them find and address any unauthorised IT activities quickly. With better visibility, they can look for unauthorised usage and take appropriate actions to bring it under control.
- **Standardised IT solutions:** MSPs typically implement standardised solutions. By offering a range of approved and secure applications and services, employees are less likely to seek unauthorised alternatives. Standardisation helps ensure that all IT resources are properly integrated, reducing the risk of compatibility issues and duplicated investments.
- **Security and compliance enforcement:** MSPs prioritise IT security and compliance. They implement robust security measures to protect data, networks, and applications from potential threats. This reduces the likelihood of data breaches and potential compliance violations.
- **Support and maintenance:** MSPs provide support and maintenance for IT infrastructure. This means catching the problems before they escalate. So employees are less likely to look for their own solutions in shadow IT.
- **Scalability and flexibility:** MSPs are equipped to handle the organisation's growth and evolving infrastructure needs. As the company expands, the MSP can grow IT services accordingly. This again reduces an employee's need to look elsewhere for solutions.

By using the expertise and services of a fully-managed MSP, an organisation gains a strategic partner in managing its IT infrastructure. The MSP's focus on security, standardisation, processes and support reduces the need for shadow IT by employees.

Your hero – a managed cloud solution

Keeping your data safe, checking your IT is up to scratch, communicating with employees and running a business can be a complicated juggling act. A managed cloud solution will take those off your hands.
With Fasthosts Proactive, your data security is our responsibility. We'll regularly monitor and check your tech for data breaches, vulnerabilities and gaps in your security and fix them before you even know about them. You can focus on running a business, while we keep everything safe.

Any questions? Our expert support team is here for you. Just give us a call on 0333 111 2000.